

REMARKS

In accordance with the foregoing, claims 27, 28, 32, 33, 37, 38, 39, 40, 41, 42, and 43 have been amended. Claim 44 has been cancelled. Thus, claims 27-43 are pending and under consideration.

On page 2 of the Office Action, claims 28 and 33 were rejected under 35 U.S.C. § 112, first paragraph, due to the claims allegedly not being enabled by the specification. Applicants respectfully submit that currently amended claims 28 and 33 are both enabled, as is clearly indicated by Fig. 2B and text of the specification, at page 13, line 13 to page 14, line 17. Withdrawal of the rejection is respectfully requested.

On page 3 of the Office Action, claims 27 and 33 were rejected under 35 U.S.C. § 112, second paragraph, as allegedly being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicants regard as the invention. Applicants have addressed the rejection by amending claims 27 and 33. Withdrawal of the rejection is respectfully requested.

Claims 27, 32, and 37-44 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Pat. No. 5,299,197 (Schlafly) in view of U.S. Pat. No. 6,157,721 (Shear).

Schlafly is directed to a protocol that applies to a computer acting as a database server, several other computers acting as terminals, and a communications line connecting them. According to Schlafly, digital information is transmitted back and forth between the server and a terminal asynchronously. See Schlafly, column 2, lines 23-28.

Shear is directed to techniques for protecting secure computation and/or execution spaces from unauthorized load modules or other executables or associated data. See Shear, column 4, lines 51-56.

According to the present invention, as defined by claim 27, for example, a first one-way function is applied to *each of a plurality of data divisions* using a first key to obtain a first authenticator, a second one-way function is applied to each of the data divisions using a second key to obtain a second authenticator, and a plurality of authenticators including the first authenticator and the second authenticator are appended to information to be authenticated. See Figs. 2A and 2B and accompanying text of the specification, at page 12, line 5 to page 15, line 11. In other words, in the present invention, the data divisions are used for creating each authenticator, as illustrated in Figs. 2A and 2B, where each one-way function differs in a key used.

Applicants respectfully submit that neither Schlafly nor Shear, taken alone or in combination, teaches or suggests, “a dividing unit which divides the information into the plurality of data divisions.” Applicants further submit that Schlafly fails to teach or suggest, “an authenticator creating unit which creates a first authenticator . . . and creates a second authenticator . . . and an appending unit which appends the first and second authenticators. . . .”

On page 4 of the Office Action, the Examiner refers to column 2, lines 34 -38 and column 4, lines 47-54 of Schlafly as disclosing, “a first authenticator creating unit (server) for dividing the information into a plurality of data (packets)” and that “the authenticators are created by applying a one-way function (hash, checksum) to each of the divided data” at page 4 of the Office Action.

Contrary to the Examiner’s assertion of the above-identified disclosure, at column 2, lines 34-38, Schlafly merely describes, “The packet is an encoded body of data. It has a header from which the type and length of data can be deduced. The contents of the packets might be ordinary text. It might also be a graphics image, a file, a file fragment, or other object.” At column 4, lines 48-53, Schlafly states, “the final field [of a typical packet shown in Fig. 3] is the checksum. This is 32 bits computed from the rest of the packet serving as a redundancy check. It is also called a hash value in the literature. If it doesn’t match, the terminal can request that the packet be resent.”

In Schlafly, although the packet is arguably in sections, for example, a header, no information is provided regarding a dividing unit which divides information into divisions. Thus, Schlafly does not offer a disclosure or suggestion of “a dividing unit which divides the information into the plurality of data divisions,” as in the present invention. Further, Schlafly also does not teach or suggest, an authenticator creating unit that functions according to the language in claim 27, for example, nor an appending unit that functions according to the claim language. Schlafly also does not teach or suggest the corresponding limitations recited in the other currently amended independent claims.

Regarding Shear, as shown in Fig. 9, Shear merely discloses that each segment is signed using a corresponding digital signature. Further, in Fig. 7, Shear simply shows that multiple digital signatures 106(1) to 106(N) are created for the same load module 54.

Therefore, independent claims 27, 32, and 37-43 are patentable over the references, as neither of the references, taken alone or in combination, teaches or suggests the features of the claims. As claim 44 has been cancelled, the rejection with respect to claim 44 is moot.

Claims 29, 31, 34, and 36 were rejected under 35 U.S.C. § 103(a) as being unpatentable

over Schlafly in view of Shear in view of U.S. Pat. No. 5,604,801 (Dolan).

Dolan is directed to a data communications system in which messages are processed using public key cryptography with a private key unique to one or more users. According to Dolan, public key processing is used in conjunction with a private key. See Dolan, column 2, lines 65 to column 3, line 21.

Although Dolan teaches the use of public key processing used in conjunction with a private key, Dolan fails to teach or suggest, "a first authenticator" and a "second authenticator" created by an authenticator creating unit, as in the present invention.

Therefore, the independent claims of the present invention are patentable over the references, as none of the references, taken alone or in combination, teaches or suggests the above-identified feature, for example.

As dependent claims 29 and 31 depend from independent claim 27 and dependent claims 34 and 36 depend from independent claim 32, Applicants submit that the dependent claims are patentable over the references for at least the reasons presented for the independent claims.

On page 5, claims 30 and 35 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Schlafly in view of Shear in view of Dolan in view of U.S. Pat. No. U.S. Pat. No. 5,757,913 (Bellare).

Bellare is directed to a method and apparatus for providing data authentication within a data communication environment. According to Bellare, by the use of authentication codes, data can be securely received even though the data is transmitted over an insecure network. See Bellare, column 1, lines 60-7.

Although Bellare is directed to data authentication, Bellare does not teach the above-identified features of the claims of the present invention. Therefore, none of the references, taken alone or in combination, teaches or suggests the above-identified features of claims 30 and 35 of the present invention, as recited via independent claims 27 and 32, respectively.

There being no further outstanding objections or rejections, it is submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge

the same to our Deposit Account No. 19-3935.


Respectfully submitted,

STAAS & HALSEY LLP

Date: _____

9 AUG 05

By: _____


Reginald D. Lucas

Registration No. 46,883

1201 New York Avenue, NW, Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501